MANGALORE UNIVERSITY

DETECTION AND ANALYSIS OF JAMMING ATTACK IN VEHICULAR AD HOC NETWOTK(VANET)

FINAL SYNOPSIS SUBMITTED
TO
MANGALORE UNIVERSITY
FOR THE AWARD OF DEGREE OF DOCTOR OF PHILOSOPHY
IN
COMPUTER SCIENCE

BY
SHUBHA R SHETTY
Research Scholar
Reg No:177073803

Under the Guidance of
Dr. MANJAIAH D. H
Professor

DEPARTMENT OF POST-GRADUATE STUDIES AND RESEARCH IN COMPUTER SCIENCE
MANGALORE UNIVERSITY
MANGALAGANGOTRI-574 199
KARNATAKA, INDIA

September-2022

TITLE: "DETECTION AND ANALYSIS OF JAMMING ATTACK IN VEHICULAR AD HOC NETWOTK (VANET)"

Name of the Candidate: **SHUBHA R SHETTY**

Name of the guide: **Dr. MANJAIAH D. H**

Date of Registration: **03/04/2018**

Place of Work: **Department of Post-Graduate studies and research in computer science Mangalore University Mangalagangothri - 574199 Karnataka, India**

TABLE OF CONTENT

SL.NO	CONTENT	PAGE NO
1	INTRODUCTION	2
2	RESEARCH METHODOLOGY	3
3	ROUTING PROTOCOLS	5
4	CHALLENGES AND SECURITY ISSUES	7
5	JAMMING MODELS	9
6	EFFECTIVENESS OF JAMMING	10
7	JAMMING ANALYSIS	13
8	REVIEW OF LITERATURE	14
9	PROBLEM STATEMENT	16
10	OBJECTIVES	16
10.1	A Comprehensive Study of Security Attack on VANET	17
10.2	Adaptive Neuro Fuzzy Technique for Jamming Detection in VANETs	18
10.3	Reinforcement Algorithm based Jamming-Detection for Vehicular Ad Hoc Networks	23
10.4	Traffic Jam Detection Using Regression Model Analysis on IoT-Based Smart City	27
10.5	Comparison of different AI based Techniques for the detection of Jamming Attacks in VANETS	30
11	PUBLICATION WORK DONE	32
12	CONCLUSION	33
13	FUTURE SCOPE	33
14	REFERENCE	34

1. INTRODUCTION

An ad hoc network is a Local Area Network, which voluntarily forms connection when devices connect. Hence Vehicular ad-hoc network (VANET) is a distinct type of ad-hoc network that can be used to improvise vehicle safety, upgrade traffic efficiency, and provide information and entertainment on go[1]. VANETs came into existence in 2001 under "car-to-car ad hoc mobile communication and networking" applications, where network is established and information broadcasting takes place between cars. Communication between vehicle-to-vehicle and vehicle - to roadside devices exist to implement road safety, map-reading and transport related services with entertainment. VANET is a prominent aspect of the intelligent transportation systems (ITS) structure. Many a times VANETs are referred as Intelligent Transportation Network.

Major global issues like road accidents, congestion, fuel consumption, and environment pollution has led to Vehicular ad hoc networks (VANETs) popularity in latter-years. Intelligent Transportation Systems (ITS) introduced VANETs to design a risk-free infrastructure for road transportation. VANETs concentrates on road safety and systematic management of traffic for roads, with bene ting entertainment and comfort to both driver and passenger. Communication between vehicles in VANETs can be attained by exchanging information using Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. Inter- vehicle communication is established using On-Board Units (OBUs) resulting in Mobile Ad Hoc Networks (MANETs) that authorizes wireless communication entirely in a distributed approach, communicating with Roadside Units (RSUs) inan infrastructure style. The Wireless Access in Vehicular Environment (WAVE) protocol established on IEEE 802.11p standard and provides basic radio standard for Dedicated Short-Range Communications (DSRC) operating within 5.9 GHz frequency band [2]. Be- low figure demonstrate the general architecture of VANET.

VANET has two wireless point with to and fro communication among themselves sharing information related to traffic, amusement and many more [3]. Two units that serves two-waycommunication are as follows:

- Road-Side Units (RSUs): Fixed mount-kind of infrastructures established either side ofthe road. RSUs furnish coverage to disseminate, exchange, and forward informationbetween nodes. Most importantly RSUs are the units that disperse safety messages within their coverage area.
- On-Board Units (OBUs): Vehicles with OBUs are capable of exchanging messages on roads. ie, Packets are transferred between the vehicles with the help of OBUs. Messages can be diverse, they can be either safety related or application-based service message[4]. When these two wireless nodes (RSUs and OBUs) are combined, two types of bidirectional communications take place in VANET: Vehicle To Vehicle(V2V) and Vehicle To RSU (V2R).

.

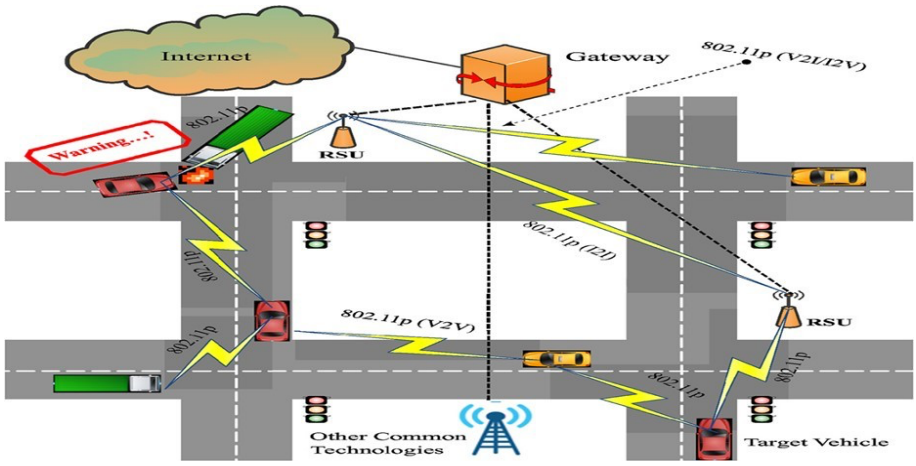


Fig 1: Architecture of VANET[5]

VANET has distinctive characteristics as compared to other mobile ad hoc networks. The unique properties of VANET not only provide vivid functionalities but are challenging as well [6]. Following are few of the attributes of VANET:

- Instantly changing network topology
- Limitless network proportions
- Continuous information interchange
- Communication Broadcast
- Time Critical
- Sufficient Energy

2. RESEARCH METHODOLOGY

Knowledge production within the field of business research is accelerating at a tremendous speed while at the same time remaining fragmented and interdisciplinary. This makes it hard to keep up with state-of-the-art and to be at the forefront of research, as well as to assess the collective evidence in a particular area of business research.

A literature review illustrated that workshops are discussed according to three different perspectives: workshops as a means, workshops as practice, and workshops as a research methodology. Focusing primarily on the latter, this paper presents five studies on upper secondary and higher education teachers' professional development and on teaching and learning through video conferencing. Through analysis and discussion of these studies' findings, we argue that workshops provide a platform that can aid researchers in identifying and exploring relevant factors in a given domain by providing means for understanding complex work and knowledge processes that are supported by technology (for example, e-learning). The approach supports identifying factors that are not obvious to either the participants or the researchers prior to commencing the workshop process.

Quantitative research is the widely used methodology in science and is also the dominant methodology used for investigative studies in social sciences and management. Generally, quantitative methodologies use the positivist paradigm. And at the same time, the socialscience researchers have experienced frustration with the positivist/ quantitative paradigm (Kuhn, 1996). The primary reasons for dissatisfaction with quantitative methodology are as follows:

The quantitative techniques use too few variables and are context neutral, that is, they do not take

into account the context. Hence, they are less suited for social science compared to physical science (Barr, 2004; Gall et al., 2003). • Quantitative researchers are focused on similarities between firms and ignore the differences among them. But researchers have often found that differences between firms are as important as the similarities (Barney, 1991; Wernerfelt, 1984). • The quantitative method is grounded in a positivist framework and disregards the individual and collective biases of the researchers as well as the subjects (Onwuegbuzie and Leech, 2005)

On the other hand, recent times have seen an increased interest in qualitative research (Denzin and Lincoln, 1994). This growing interest in qualitative research can be seen by the numerous high-quality studies that are being done using qualitative methodologies as well as the increasing number of special issues on qualitative research in highly ranked strategy and general management journals (Ridder and Hoon, 2009). Though qualitative methodologies address many of the above limitations of quantitative methodology, there are concerns related to standards, validity, reliability and rigour in qualitative research (Flick, 2007; Frankel, 1999; Gibbert et al., 2008; Seale, 1999). The most important concerns among them are as follows: • Lack of rigour: Many hold the view that nonpositivist inquiry is more craftsman-like and less scientific. To avoid this criticism, there is increasing focus on improving quality on both data collection and data analysis (Ridder and Hoon, 2009). To boost the data collection process, researchers are focused on enhancing the quality of single data collection techniques as well as possibility of using complementary data collection procedures (Flick, 2007; Seale et al., 2007). Data analysis helps the researchers to reach theoretical contribution from raw data by transforming, inter

preting or making sense of qualitative data (Mahoney, 2004). The inadequate development in this field, particularly in respect to techniques and procedures for analyzing data is a significant barrier in theorizing with qualitative data (Gephart, 2004), • Little basis for generalization: Qualitative research are embedded in the context; hence, many assume that it would be difficult to generalize. The qualitative researchers also work with a very small database. Thus, moving from that data to general theory often elicits a ‘So What?’ or ‘What Else?’ response (Stake, 2005). • Practical difficulties: Qualitative research is time consuming when it comes to data collection, data analysis and creating research reports. It also calls for extended field work, getting access to site, handling massive documentation and significant time commitment compared to either survey or secondary data source-oriented positivist quantitative enquiry (Atkinson and Delamont, 2006). With the above background, we have been able to establish the key arguments in favour of and against both the methodologies. The purpose of this article is to review the following: • First, the distribution of qualitative and quantitative methodologies based on the number of articles published in top strategy and general management journals. • Second, as qualitative methodology is pluralistic, conducting an in-depth analysis of evolution of methodologies and trends in qualitative research during this period. And based on the above analysis, our study assesses and presents the areas where qualitative methodology would be more suitable for strategy researchers and particularly in the context of Indian business.

Research Design The research design for this survey involves identifying top rated strategy and general management journals and reviewing the published empirical articles for diversity and evolution related to paradigms and methods. For identifying journals, time frame and actual paper, we have opted for the structured selection approach that was used by Dibbern et al. (2004) in their article ‘Information Systems Outsourcing: A Survey and Analysis of the Literature’ for selecting the research articles for this study. According to them, the ‘selection process’, that is, how the research papers were chosen, had three phases: journal selection, time frame selection and paper selection.

3. ROUTING PROTOCOLS

With the help of various communication variant vehicles on road exchange diverse information over the network. Therefore, information dissemination plays prominent role in VANET. Role of routing protocols comes into picture when information propagation takes place between vehicles and roadside infrastructures. These protocols are standards or conventions that decides regarding packet routes between different nodes. Hence designing a dynamic routing protocol, itself is a challenge due to changing networktopology in VANET [7]. Routing protocol can be classified based on topology, position, broadcasting, clustering and geocasting.

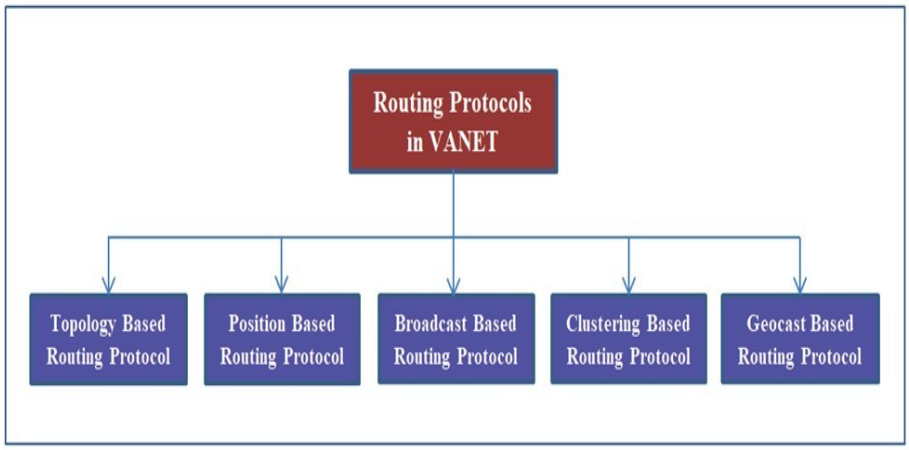

Routing Protocols in VANET
Topology Based Routing Protocol
Position Based Routing Protocol
Broadcast Based Routing Protocol
Clustering Based Routing Protocol
Geocast Based Routing Protocol

Fig 2: Classification of Routing Protocol in VANET[7]

- **Topology Based Routing Protocol**: This protocol depends on the topology of underlying network. It maintains a routing table. It uses store and forward methodology. Its performance is slower compared to other type of routing protocol. There are two types of topology-based protocol, they are Proactive routing protocol and Reactive routing protocol. Examples are: FSR (Fisheye State Routing), DSR (Dynamic State Routing).

- **Position Based Routing Protocol**: This is even called as geographic based routing. It makes use of GPS services for routing. It is promising method compared to rest of the routing techniques. It uses greedy forwarding to share messages and optimal path. Examples are CAR (Connectivity- Aware Routing), Vehicle Assisted Data Delivery (VADD)

- **Broadcast Based Routing Protocol**: This routing technique is used in emergency like accident etc. Messages can be delivered beyond the transmission range. Flooding mechanism is made use of to guarantee packet delivery, but results in excessuse of bandwidth. Example: BROADCOMM, UMB (Urban Multi-hop Broadcast), ZRP (Zone Routing Protocol), V-TRADE (Vector-based Tracking Detection), HV- TRADE (History Enhanced-TRADE)

- **Clustering Based Routing Protocol**: The protocol allocates the point of network with various intersecting or decomposed clusters in a di used manner. cluster head is selected to communicate with different cluster heads or cluster nodes. Example: COIN (Clustering for Open IVC Networks), HCB (Hierarchical Cluster Based

routing)

- **Geocast Based Routing Protocol**: It is a modification of multicast technique, where packets are transferred to every node within a predefined geographical region. It guarantees low-cost packet delivery. Example: ROVER (Robust Vehicular Routing),IVG (Inter-Vehicular Geocast)

CHALLENGES AND SECURITY ISSUES

VANETs has distinguish features like mobility constraints, infrastructure-less architecture, and frequent loss of network connections between nodes. All these constitutes to serious network security threats. Hence developing secure algorithms which promotes safe network communication and provide better security is a challenge [8].

Security attacks on Vehicular ad hoc network can happen in several forms. There are variety of attacks. A professional or nonprofessional attacker will organize an attack using variant strategies. Few attacks are on packets, where a packet may be dropped, delayed, or may be forwarded to false destination. Numerous attacks are done to alter existing data by adding or deleting or injecting false data in a packet. Which results in network chaos and may end up with life threatening scenario like road accident. Furthermore, few attacks may hamper different technologies in VANET that will tamper VANET functionalities [9].

Purpose of launching an attack in VANET may be due to numerous reasons. Few attackers perform attack just to eavesdrop the conversation over the network, some may intend to damage information sent on packets across the network.

Various research has classified attacks based on various parameters. Figure 3 shows different categories of attack and their subcategories as well. In the foremost category authenticated users identity information is used to launch the attacks by the at- tackers. Second group of attack is based on sending faulty or adjusted piece of information. Group three is about prolonging or eliminating necessary packets or sending those packets to diverse destined user. Group four is a type of attack to clog or gather messages that are conveyed in the forum. The last group of attack is to hamper VANET architecture.

- **Availability Attack**: It consists of Denial of Service (DoS) attack, jamming attack, Greedy behavior, Broadcast tampering, Malware attack, Spamming, Black-hole attack and others are those attacks that avert the network to function in normal mode, making the service of communication channel unavailable. This kind of attacks denies the users with the network privilege and services. They may take various forms like jamming communication channel and hindering the delivery of safety related messages to the user. DoS attack can be accomplished through various other attacks like jamming, Black-hole attack, Greedy behavior, Grey-hole attack, Warm-hole, Malwareattack etc.

- **Authentication and Verification Attack**: Attacks under these categories are evident throughSybil attack, replay attack, GPS spoofing, Position faking, Masquerading, Tunneling and others. Malicious node may hold duplicate or many identities which creates erroneous message or may fake congestion. Faking with position, speed or even location and curbing the safety on road is the foremost intention of these attacks.

Confidentiality Attack: It is all about the true owner who has the right to access the information. But attack on confidentiality will hinder the purpose. Eaves- dropping, information gathering, and tracking are the various forms of confidentiality attack. Where an attacker might deliberately overhear the confidential communication that takes place on a communication channel and misemploy. Encrypting the confidential data over the network may to some extend put a stop to privacy violation

- **Integrity and Data Trust Attack: S**ending and receiving the original and authenticated message is integrity and data trust. However here attackers try to hamper the integrity of data through numerous forms such as masquerading, fabrication or altering data, suppressing messages, replaying and so on. In masquerading attack, the con- tender fakes his identity as a legal source and disseminate fallacious message. Likewise fabricating attack transgress security requirements such as nonrepudiation and integrity. Sole intention of fabrication attack is to alter the original data and disperse bogus message throughout the communication channel

- **Nonrepudiation/ accountability attack**: Attacker here make it tedious to keep an accountor trace of numerous events that takes place in a network which are essential for safety on road [10].

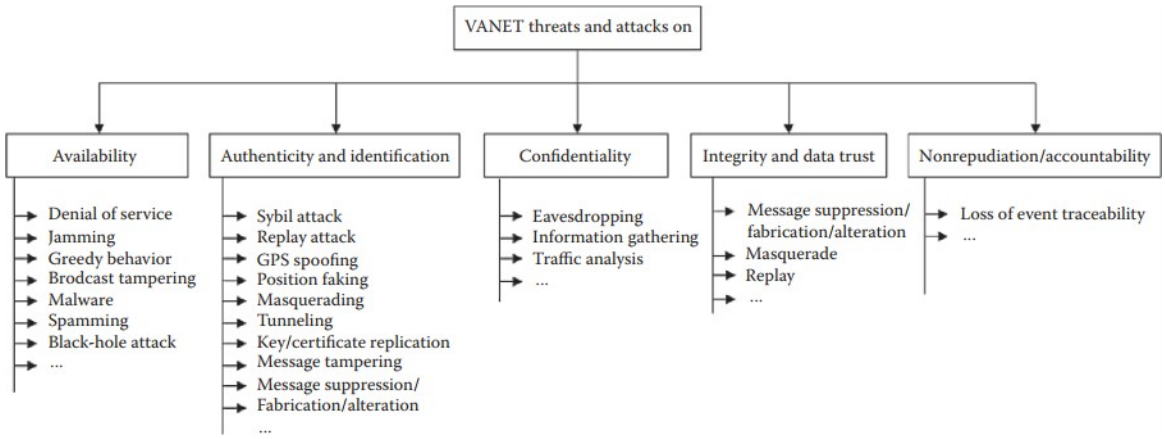


Figure 3: Classification of Attack

VANET is ad hoc in nature, this wireless communication is prone to various attacks leading to tampering of data privacy, integrity and confidentiality which becomes an obstacle to VANET application. Hence attackers and attack launched by them are major concern when security comes into picture. Attackers can be grouped based on who the at- tackers are, their intension of attack, impact of attack on VANET, and whether the attack is bounded or not. The following are the classification of attackers based on below variable:

- **Insider vs Outsider**: Insider is the one who is a genuine member of VANETs launchingan attack on the network whereas the outsider is the non-genuine member

- **Malicious vs Rational**: Malicious attacker is non beneficial attacker while rational attack is intended one

- **Active vs Passive**: Active attacker are the one who generates recent packets or destroy packets that are already used in the network however passive attacker only intrude the wireless transmission.

- **Local vs Extended**: Local attackers can launch an attack locally i.e., within specific boundary, while extended attackers can launch an attack beyond the network access.

Based on the types of attacks and attackers jamming attack is considered as matter of concern and has become a research topic as well. Jamming attack is one such attack that occurs when jammer consciously sends radio signals to distort the communications by minimizingthe signal-to-noise ratio. The term jamming is made use to differentiate it from coincidental jamming which called interference. Here we aim to examine Jamming attacks which is launched to damage communications purposefully. Hence, we need to understand jamming strategies performed by various jammer [11].

Jamming attack can be organized into four dissimilar groups depending on their behavior. They are Constant, Deceptive, Random and Reactive jamming.

- Frequently imparting undirected information on the medium irrespective of state of the medium (Idle or not) is constant jamming.
- Continuously introducing a stream of undirected information with no space between consecutive packets carried out in a network is deceptive jamming.
- Fluctuation between jamming and sleeping process to preserve energy is random jamming.
- Reactive jamming happens only when the communication channel is busy and active which is other case comes to idle state.

4. JAMMING MODELS

Jamming attack can be classified based on its mobility and its behavior exhibiting various characteristics. These variety of jamming attack has their own severity on communication channels, at times may be life threatening too. Jamming attack can be modelled as follows

- **Mobility**: Assuming that jammer has restricted transmission power and can only affect its neighboring communications, a jammer may target an RSU, a stationary unit, even an OBU which is nonstationary unit, or randomly keep moving. To model these jamming patterns, we consider the following jammer's mobility pattern concentrating on highway roads, where jammer stays undetected.

- **Stationary:** In this case a jammer may reside inside stationed vehicle or positioned on the sides of road. This type of jamming can only affect the same area effectively where jammer is located. Here jammer has over all control on location selection, but jammersare restricted to stay stationary since it's in a highway road.

- **Targeting mobility**: Here jamming is target based. A specific node (vehicle) is targeted, and radio signals are continuously transmitted in its communication channel. Jammers make sure that they stay close to the coverage area of a car throughout the jamming session. Due to the adoptive jamming behavior, this type of jamming is hard to detect especially when it combines with reactive jamming behavior.

- **Random mobility**: In this type of jamming a jammer reside in a vehicle and keep moving randomly on road. They are capable of manifesting random and high mobility, but they are restrained with road limits. Randomness makes these kinds of jammers go undetected.

- **Behavior:** In inclusion to mobility pattern jammers can even exhibit various behavioral pattern too. They are as follows:

  - **Constant**: A constant jammer is the one who constantly and randomly sends radiosignals in a channel without being constrained to any MAC protocols. The goal of thisbehavior is not allowed authorized vehicles (nodes) to access the communication channel to send packets. In order to falsify the packets by creating high interference causing high bit-error-rate (BER) at the receiving node resulting in constant drop of packet rates.

  - **Random**: In this behavior of a jammer energy consumption comes into picture, be-cause to launch a jamming and to inhibit communication between nodes consumes massive energy. Hence to cut o energy consumption a jammer sets timing(t) between sleepmode(tS) and jam mode(tJ) in seconds. The jammer switches between these two modes, permitting the jammer to have more grip on power consumption as per his requirement.

  - **Reactive**: This jamming condition does not focus on corrupting packets at sender's end, instead these sophisticated active jammers concentrate on receivers. They persistentlyoverhear the targeting communication channel, once packets are sent from transmitting node the jammers repeatedly hamper the packets at the receiving node. Detecting this kindof jamming is a tedious job since jamming signals overlap with the packet transmission.

5. EFFECTIVENESS OF JAMMING

Jamming attack is one such security threat to the vehicular ad hoc network that can make a serious impact on the network most of the time it may result in fatalities. To detect jamming in a network it is must to study the impact made by the jamming attack with severity and ultimate result. Therefore, following three metrics can be used to realize if ad hoc network is under attack by a jammer. Below metrics tightly associated with each other and out-turn network performance [12]

- **Packet Delivery Ratio (PDR)**: The collation between incoming packets received at the end of receiver and outgoing packets from the sender is packet delivery ratio. The density of vehicles on road in VANET keeps f l uctuating depending on road condition.For example, during peak hours or peak days the traffic on road will be considerably high leading to reduced packet delivery ratio. A prominent fall in packet data ratio occurs when jamming prevails, which is caused by the noise from jamming attack.

Accordingly, reduction in PDR either due to the bottle neck in the network or dueto the jammer, is barely possible to depend on PDR alone.

- **Packet Send Ratio (PSR):** Always ratio of packets that are accomplished through an authorized user must be compared with the ratio of packets send out in MAC layer. Drop in packet send ratio can happen in two situations. Firstly, is when roads are congested, vehicle travel in lower speed and results in extended communication time between vehicles. Simultaneously, channel encounters further RTS/CTS (Request/Clear -to send) flow control signals, directing larger fall in PSR. Secondly when jamming prevails in the network, the channel will frequently tend to be busy due to the noise induced by the jammer, resulting in back-o -timer and delay in receiving CTS response. Nevertheless, roads are congested or jammed, packets will be usually discarded when new packets arrive, and when time-out occurs drop in PSR will happen. Hence PSR alone cannot be used as a tool to identify jamming attack.

- **Signal Strength (SS):** SS measures the quality of radio frequency signal sent from sourceto destination and is a high- powered tool for measurement at receiver's end. De- pending on commissioned protocol, wireless points can test SS at any point of time. SS serves a great tool for researchers to identify jamming attack in wireless network. Vehicles are free to move in VANET, where it can randomly enter and come out of communication range. Increase in SS can occur due to high vehicle density (congestion) or may be intentionally.

6. JAMMING ANALYSIS

Numerous works are carried out with regarding jamming problem choosing 802.11p communications, still no comprehensible definition of jammer's potential exist. A regular presumption about jammer is that a jammer can jam wireless transmissions with no restriction at unspecified or stable speed and jammer can proceed with no restriction. Assumption is that effect of jamming and adaptability can be closely concentrated. PDR, PSR, and SS are the network metrics that can analyze jamming and can be applied in variant scenarios like congested road, highway road etc.

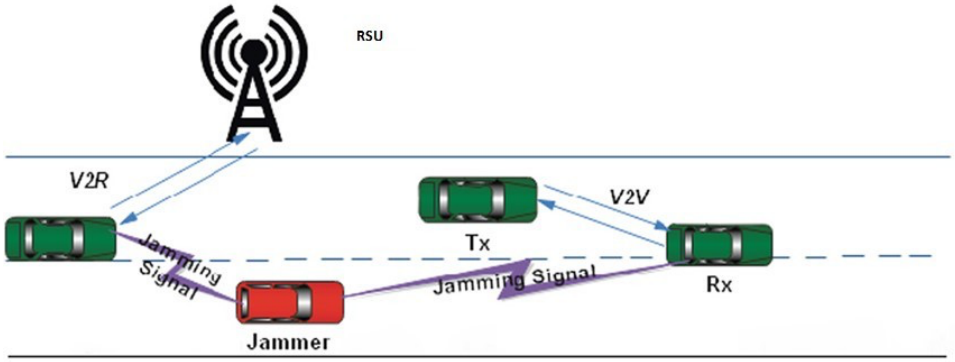


Figure 4: Jamming Scenario in VANET
[13]

7. REVIEW OF LITERATURE

VANET being widely gaining popularity has exposed to enormous security issues. Safety is prioritized and researchers worldwide are working to strengthen the wireless network security. Handling various attacks on VANET has become a challenge and jamming attack is one among them. Following are few research papers related to jamming attack that are been reviewed to intensify the research topic and objectives to be achieved.

F.Nyongesa et.al.,(2015)[14]has conducted a survey on Doppler shift compensation schemes and its provocation on VANET .The survey is conducted in high- mobility wireless network where latest strati cation consisting of six variant scheme. Compensation schemes are portioned into time domain, space domain and frequency domain. Which are further categorized as time partitioned based scheme, modulation and coding based, autocorrelated based, interference cancellation based, beam foaming based and diversity combining based. Bite Error Rate is calculated in all six schemes based on which VANET performanceis concluded.

AMS Abdelgader et.al.,(2014)[15]has concentrated on PHY layer of IEEE 802.11p standard, providing an overview of frequency band, specifications and block diagrams of WAVE PHY. Since VANET is emanating as a revolution in transportation domain, network security and privacy along with road safety plays key role. To achieve network safety focusing on PHY is prime consideration.

Lv Humeng et.al.,(2012)[16] proposed The Distributed Beacon Frequency Control Algorithm for Vehicular ad hoc Network, which will redesign by adjusting frequency of beacon messages in two different instant. The proposed algorithm can detect and calculating network burden. It can control the frequency of beacon messages that are sent at each time interval depending on the domain. To deal with the overcrowding caused by periodic messages half the frequency every time method is acquired. The algorithm is practically simulated using NS2 simulator to check the performance in heavy traffic condition and proved that beacon receiving probability has increased due to effectively making use of bandwidth.

Yi Qian et.al.,(2012)[17] has designed productive medium access control(MAC) protocol in order to well-timed message diffusion in VANET, which in turn enhances network security and road safety .This proposed protocol is designed for various kind of applications with variant messages of prime concern so as to access DSRC channels. Through simulation proposed protocol is potential enough to furnish secured communication with reliability, less latency, integrity, non-repudiation, privacy of the source or the sender.

Huong Nguyen-Minh et.al.,(2015)[18] has proposed a jamming detection technique to detect loss of packet that takes place either through jamming attack or accidentally. A systematic model is even launched to review the productivity and accuracy of proposed system. It is specifically used to detect reactive jamming directing beacon messages. This system is operated on multi-channel, where VANET receives both safety and non-safety related messages.

SO tengstrand et.al.,(2014)[19] has surveyed the radio signal obstruction to study the system performance and even its influence on the IEEE 802.11p system where bitrate, packet delay and packet error possibilities are taken into account. As known the VANET system is built on ARQ (Automated Request Repeat) and Carrier Sense Multiple Access (CSMA)problem related to interference is closely associated, which may happen aspacket delay on constant rate of data. Hence radio signal interference problem exists as a challenge in nearest future when it comes to safety or non-safety related messages. Threedifferent types of radio signals are studied such as Continuous Wave (CW), Pulse modulated sine signal and Additive White Guassian Noise (AWGN). On IEEE 802.11p CW has very bad mortification when normal spread noise AWGN. Pulse modulated sine signal is considered to have lesser signal degradation compared to all the three. But ignoring this degradation is not the solution instead duty factor of the signal obstruction should be considered. Measuring only the RMS (Root Mean Value) of the signal interference is nota good practice. Using Impulsiveness Correction Factor (ICF) can be one among possible solutions to this problem. When time critical events like safety applications are considered,delay plays prominent role. Hence radio system must be wisely selected depending on typeof applications we are working on.

Ali Hamieh et.al.,(2009)[20] has projected a model which is capable of recognizing distinct type of jamming attack only when jammer communicates through workable radio signals radiate from its device. The model is constructed on the quantity of distribution of errors. VANET is largely prone to denial-of-service attack, and it becomes important to detect the attackers and kind of attacks done. Relying on calculations done between the correlation that prevails in the middle of errors and the receiving time to find the existence of jamming attack in VANET the new detection model is established. Simulation results are capable of detecting jamming in initial credentials.

RS Raw et.al.,(2013)[21] a review on VANET security issues and numerous challenges prevailing in ad hoc network which hinders the free owing communication amongst vehicles on road. A close observation is done on diverse attacks and solutions for the attack thattakes place on VANET. Dissimilar variables are examined to make a comparison between solutions. Mechanisms that are used to solve attack issues are even highlighted.

N Lyamin et.al.,(2014)[22] has presented latest model to detect Denial of Service(DoS) attack vehicular ad hoc network with communication standard IEEE 802.11p.Platooning scenario is considered and a straightforward algorithm is developed for identification real-time jamming of timely positioning beacons communicated among vehicles on road in group. Likelihood of detecting jamming and fake signal is evaluated among two dissimilar attacker frameworks. Simulated result shows the probability of detection is not less than 0.9 and no fake signaling probability for any jamming too.

IK Azogu et.al.,(2013)[23] brought forward a hideaway scheme acceptable for anti-jamming in vehicular ad hoc network. To analysis the effectiveness of jamming a new security measurement standard is recognized and employed to design protection structure. The calculations and communication function are done through road side unit rather through onboard unit. The output through simulation clearly shows that the presented system is more capable of improving VANET efficiency against jamming in comparison

with traditional system such as channel surfing. The new system is likely to be a defense mechanism.The road side unit is variedly and efficiently used in the new model.

A Aijaz et.al.,(2006)[24] made an introduction to prototype of attacks that happens on communication between vehicles. This framework is used to clarify system archetype of NoW(Network-on-Wheels) communication system. And this model is even used to discover possible deficiency of NoW communication system during its specification stage. Thework even came across few strongly unrecognizable attacks on various units such as hard-ware, software and even sensors. Certain fascinating issues and challenges which require insight focus too are highlighted here. The attack tree serves as a key to analyze the system security. To magnify the complete security two mechanisms were found worth. Two mechanisms are plausibility check conducted in cars and regular system check specifically on roadside units. Collation between message received and inner sensor data, even assessing messages from diverse source of information based on sole event and constructing structures in relation with unique traffic events that are associated with facts is plausibility check. Though simulation results in enlarging e orts of attackers but variety of application need to deal properly with some other models. A genuine verification of working of each device is done through regular system check resulting is less defection in any units and can be employed to update the software as well.

A Benslimane et.al.,(2017)[11] has introduced new analytical model to investigate the e effectiveness of reactive jamming attack and the impact of jamming on broadcasting. The proposed system can distinguish the performance of network during normal network scenario and jammed situation. To accomplish safety associated applications in VANET a detection methodology based on MAC is proposed which overpower thethreshold method used in detection task. The proposed system can more precisely differentiate the reason for collision between contents, jamming attack and interventions. With the help of reduced possibility of fake alarms jamming attack detection is simplified. Simulationresults and calculations are used to assess the detection system. Fake alarms are possibly sidestepped to increase the execution of detection method. The detection method- ology is investigated in both platoon situation and normal environment. The algorithmhere shows better performance in platoon environment where vehicle count is stable andmonitored using technology related to platooning.

M Sun et.al.,(2017)[25] presented a new data trust scheme that can wisely discover the trustworthiness of a message on the network and is capable of distinguishing erroneous information. Paradoxically it can reliably tack the vehicles on the road despite of messages being reported imprecisely. Through the wireless physical layer, effect of reported vehicles information with the help of reliable sensor techniques are sensed which is the ultimate concept behind this model. This mechanism is tied within a vehicle tracking system which is dynamic in nature, for which extended Kalman alter is made use of. Chi-Square trial is made use of to determine fallacious information. Simulation results are highly productive when highway traffic scheme with less pointed curves is taken into consideration and when a genuine neighboring vehicle exists.

MA Karabulut et.al.,(2017)[26] has developed a logical scheme to evaluate the performance of IEEE 802.11p Enhanced distributed channel access function (EDCAF)for vehicular ad hoc network. The association among performance factors and EDCAF factors

are obtained. The conceptual analysis is made using 2D Markov chain model. The Markov chain model examines all the prime matrices which makes an impact on the IEEE 802.11p performance. Those factors comprises of background counter freezing, qCW[QC](contention window),AIFSN[QC](arbitration inter-frame space) etc. Simulation is carried out using this performance scheme. Packet drop ratio, throughput and latency time are acquired.

M Raya et.al.,(2007)[27] has proposed a scheme that recognizes the most applicable communication features. A secure framework along with associated protocols. Necessity ofsecurity on vehicular ad hoc network and privacy issues are focused.

S Zeadally et.al.,(2012)[28] has surveyed current research issues such as qualityof service(QoS), routing protocols, broadcasting with respect to vehicular ad hoc net- work. Standards for wireless access has been reviewed, where trails and major deployments in various parts of the world is studied. Various vehicular ad hoc network simulation tools like simulators are examined, with respect to their performance, efficiency etc. Research related challenges with respect to VANET is highlighted.

MS Mohamed et.al.,(2017)[29] has examined hybrid jamming attack in vehicularad hoc network and presented an enhanced voting algorithm for the same. To in- crease the reliability of the network voting-based scheme is implemented, where influence of hybrid jamming on voting-based perspective is explored. Practical examination depending on attack model is conducted with the help of devices such as onboard unit that are available commercially. The newly presented algorithm has high-ranking with respect to the amount of time taken to decide the reliability. EEBL application is made use of during the experiment as an example. The time making decision has been advanced to 3.3 seconds during the experiment, which is a great leap because for those messages which are safety oriented every second makes a difference. Safety messages are time critical nd may end up being fatal if delayed.

C Chen et.al.,(2009)[30] has brought forward a robust sybil attack detection(RobSAD) mechanism depending on normal ow of vehicle and even on suspicious move. Considering restricted architecture of vehicular ad hoc network attack on each node can de independently perceived by interrelating digital signature of neighboring vehicles. The result of simulation proves that the presented framework performs outstandingly with less network requirements, as well as reduced rate of detection, hands overhead efficiently and is robust.

N Panjrath et.al.,(2017)[31] has made a brief study on vehicular ad hoc network concerned with its architecture, security issues and design issues. A survey on VANET's communication system is even pursued. Various hardware, software and sensor units are deeply studied. Ad hoc network supports variant routing protocols which are analyzed in this paper. An insight on communication domain of VANET is made to support the

8. PROBLEM STATEMENT

Jamming is a consequential threat to VANET security. Jammer frequently sends signals (in pretentious zone) to hinder the communication between nodes in the network. Jamming attack keeps the communication channel busy and the victim feels the same. Hence jammed node neither can send nor receive information from the effected region. When jamming is exhibited, the sender can a frequently send packets without any intermission, while receiver may not receive the same. Therefore, packet delivery ratio (PDR) comes done. These packets may transfer vital information (life threatening) like, road conditions, weather, accidents, etc. And failing to receive such packets may lead to endangerment

Since VANET has high mobility and rapid changing network topology defending it against jamming attack is a challenge. The jammer is not abided with any protocol and their mobility is unrestricted. Besides, challengers have over all control on starting a jamming and going to sleep mode so that they can obscure their existence. Amalgamation of all these issues has made jamming hard to detect and solve.

Making a note of above issues hindering normal communication flow between vehicles in ad hoc network, making a thorough study of existing jamming detection mechanism and their performance factors is essential. Based on the existing detection techniques weare focusing on developing a jamming detection model that is more effective in detecting jamming attack in VANET.

9. OBJECTIVES

I. **Investigating detection mechanisms for jamming attack in VANET.**
Several jamming detection techniques are built in order make smooth functioning of ad hoc network, hence studying these existing techniques plays a crucial role in better understanding the problem.

II. **Performance analysis of detection techniques for jamming attack.**
Every developed model has its own performance factor that shows how effectively it works and to what extend the mechanism can handle the problem. Therefore, analyzing the existing jamming detection mechanism is done to build the better version.

III. **Developing a model for detecting and distinguishing jamming attack in VANET.**
Once existing detection frameworks are deeply studied with their performance factor and working pattern, a new model can be developed with enhanced performance. The new model must detect the jamming attack and differentiate it.

IV. **Comparative analysis of jamming attack detection technique.**
To show the newly constructed model is much effective than already existing one, a comparative study of new model with existing techniques need to be done, which will show how strong and effective is the newly built model in detecting and distinguishing jamming attack in vehicular ad hoc network.

9.1. A Comprehensive Study of Security Attack on VANET

The first objective "Investigating detection mechanisms for jamming attack in VANET" is achieved through the paper titled "A Comprehensive Study of Security Attack on VANET" . In this paper we discussed the outline of VANET through its framework. The basic model of VANET is studied to understand the service system in VANET. Standards of VANET is even reviewed, which is the backbone of vehicular services.

Followed by the type of communication in VANET and routing protocols. A broad study on various security attack and attacker is done to understand the security issues associated with the wireless communication. Focus on jamming attack and its effectiveness is thoroughly analysed with the help of different parameters. In addition, future scope of research associated with jamming attack and possible developments are considered.

9.1.1. Conclusion

VANET is promising technology for vehicular communication network, due to its extensive applications and vivid safety related services. It has undoubtedly become a topic of research in the field of automobile, educational institution etc. Due to gaining popularity of VANET, Security has become major concern. After analysing various attacks, jamming seems to be a challenging task. Maximizing road safety and minimizing jamming attack on vehicles, is the major concern. Jamming is a consequential threat to VANET security. Jammer frequently sends signals (in pretentious zone) to hinder the communication between nodes in the network. Jamming attack keeps the communication channel busy and the victim feels the same. Hence jammed node neither can send nor receive information from the effected region. When jamming is exhibited, the sender can affluently send packets without any intermission, while receiver may not receive the same. These packets may transfer vital information like, road conditions, weather, accidents, failing to receive such packets may lead to endangerment.

VANET has high mobility and rapid changing network topology, defending it against jamming attack is a challenge. The jammer is not abided with any protocol and their mobility is unrestricted. Besides, challengers have over all control to start a jamming attack and go to sleep mode so that they can obscure their existence. Amalgamation of all these issues has made jamming hard to detect and solve. Making a note of above issues and the review done. Our further research focus on studying existing jamming attack and its effectiveness and trying to develop a jamming detection model that is more potential enough in detecting jamming attack in VANET.

9.2. Adaptive Neuro Fuzzy Technique for Jamming Detection in VANETs

This paper concentrates on second objective of the research "performance analysis of detection techniques for jamming attack". In this work adaptive neuro fuzzy based algorithm is introduced. To validate results, variables such as detection time, detection ratio, and positive false ratio are used. The outcome of the presented method is finer in comparison to existing methods.

9.2.1. Methods and Tools

The proposed work is to aim at the deep learning-based Adaptive Neuro Fuzzy Interface system (ANFIS) to obtain the security index in the vehicular network. In this method, initially trained data is used internally with neural networks and output is given to the fuzzy logic to detect the index of attacks.

9.2.2. ANFIS Theory

It is mixture of ANN with fuzzy interface system. The Takagi - Sugeno model is used in this proposed work [13]. ANFIS is a very good learning technique to take over an issue on uncertainties in any system. This controller is based on framing fuzzy IF-Then rules that produces specific input-output with the help of membership functions. The learning process of ANFIS consists of three stages; first is the rule base, second is the membership functions and the third is the reasoning mechanism [13]. The Fuzzy Rules in the form of Equations is given in below.

If Vj= If x_1 is $A_1(x_1)$ and x_2 is $A_{2j}(x_2)$ and .....x_n is A_{nj} (x_n) THEN y is c_j. Here x_1 is considered as change in error given as w_{ref}- w_r and x_2= derivative of change in error given as d (w_{ref}-w_r)/dt.. Output is defined by the formula y = output given as $Pix_1+Rix_2+S_i$. Here input variables are called as input linguistic labels and output variables are defined ad consequent labels. The Fuzzy Interference is implemented using the Eq. (1) and Eq. (2).
The weight of wj in each rule is calculated as shown in Eq. (1)

$$w_j = \prod_{i=1}^{n} \mu_{ij}(x_i^0) \tag{1}$$

The output inference result y is obtained by means of the weighted average of the consequents in Eq. (2)

$$y = \frac{\sum_{j=1}^{m} w_j c_j}{\sum_{j=1}^{m} w_j} \tag{2}$$

Here Output is defined by 'y' and weight function is represented using w_j.
The Structure of ANFIS has have different types of interference layers which is represented in Figure 1.
Every single node generates output by solving each membership function as shown in Eq. (3). Here k_{ij} are output nodes.

$$k_{ij}^{(1)} = \mu_{ij}(x_i^0) = f(x_i^0; p_{1ij}, p_{2j}.....) \tag{3}$$

The 2nd layer has precondition of fuzzy rule and represented by 'π' which is shown in Eq.(4).

$$k_j^{(2)} = \prod_{i=1}^{n} k_{ij}^{(1)} = w_j \qquad (4)$$

The output of the jth node $k_j^{(4)}$ is shown in Eq. (5), these layer 3 has consists of m- nodes normalization layer.

$$k_j^{(4)} = \sum_{j=1}^{m} k_j^{(3)} c_j = y \qquad (5)$$

The structure of adaptive fuzzy controller, which is implemented in MATLAB is shown in Figure.6.

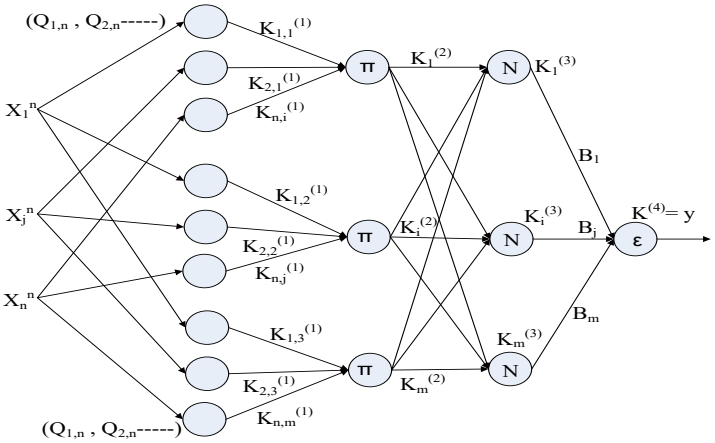


Fig. 5. Structure of ANFIS System with weight Functions [13]

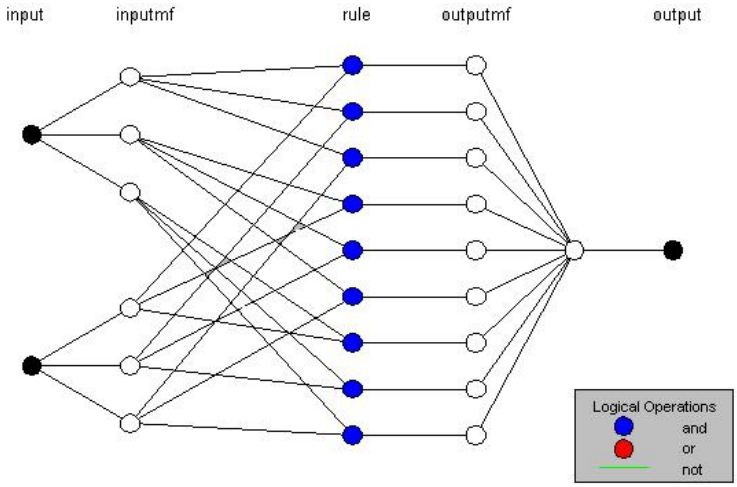


Fig. 6. Structure for ANFIS generated though MATLAB

9.2.3. Results and Explanations

In VANET, its execution with reliability has significant importance. The Proposed Method has evolved with Adaptive Neuro Fuzzy Inference controller (ANFIS). The proposed method has typical design and will give the notable detection rates.

Performance Evolution
To evaluate the proposed method, three parameters are considered: rate of detection, false-positive rate, time to detect in opposition to packet ratio, and selective forwarding attacks**.**

Detection Rate: This is the count of suspicious incident's ratio announced to the occurrences of count of suspicious incident.

DR = (malicious events Detected in total) / (malicious events in total)
If the DR is high, then the accuracy of the detection system will even increase.

False positive rate (FPR): This denotes the proportion of a fake obstruction noticed to the count of standard point.

FPR = Innocent Nodes Detected in total /standard nodes in total.
The Proposed method is compared with existing methods such as clustering algorithm [13] and results of proposed algorithm is discussed in detail with respective waveforms. The simulation parameters to execute the proposed method is shown in Table.1. To analyze the condition of the accuracy is high if FDR ratio will be less. If FDR ratio will go high, then the system has low accuracy.

Table 1. Simulation Parameters

Sl.No	References	Methodology
1	Apparatus to simulate	NetSim and MATLAB
2	Traffic Generator	SUMO
3	Range of Communication	250m
4	MAC Protocol	IEEE 802.11 p
5	Node Density	50–300
6	Simulation Area	300 m × 300 m
7	Type of Connection	UDP
8	Type of Application	CBR
9	Size of Packet	512 bytes
10	Highest. no. of Suspicious Nodes	45% of the total Nodes
11	Time to Simulate	700 s
12	Mobility Model	Manhattan Mobility Model
13	Types of Attack	Packet Drop, Selective Forwarding

9.2.4. Results

The proposed system's performance is depicted in the waveform. Figure 3 gives the performance of detection rate with the proposed method and existing clustering method [13]. As the detection rate goes high, the system will result in better performance. In the proposed system, the detection rate of ANFIS method is high, which is around 22% with approximately 50 vehicles. For high number of vehicles, the detection rate is around 98 % .Hence in comparison with existing methods, the proposed method has an elevated detection rate.

Figure.7 shows the performance of the number of vehicles with a false positive ratio for existing and proposed methods. The False positive rate is low for each number of vehicles in the proposed ANFIS Method. In contrast, current practices have a higher false-positive ratio than the number of vehicles in comparison with present work.

Figure 8 exhibits performance of detection time in the proposed ANFIS method and existing methods with the positive forward attack. The proposed method has less detection time with the number of vehicles. The clustering algorithm [13] shows the performance with high detection time. In conclusion, the proposed method manifests better performance with the above results.

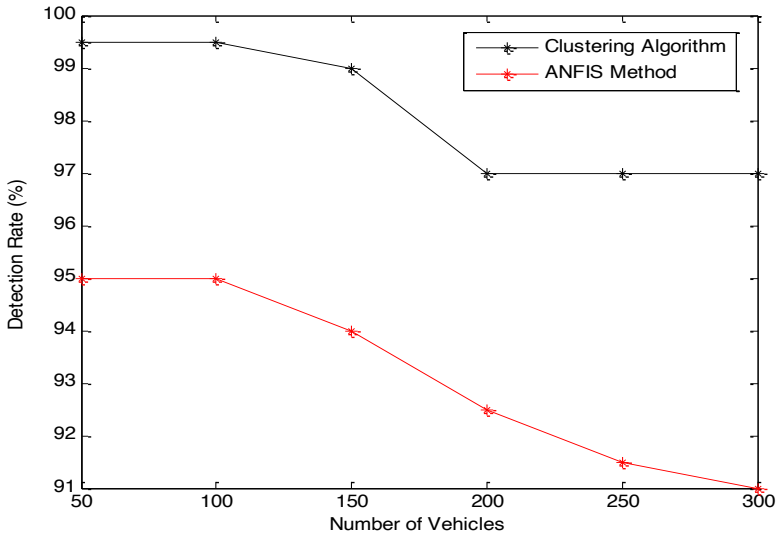


Fig. 7. Performance of Detection Rate with Proposed and Existing Method

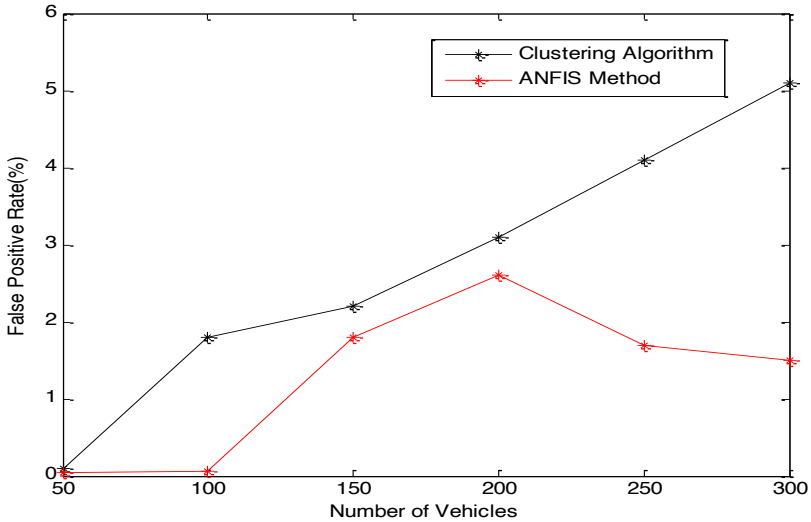


Fig. 8. False Positive Rate for Packet Drop with Number Vehicles

.

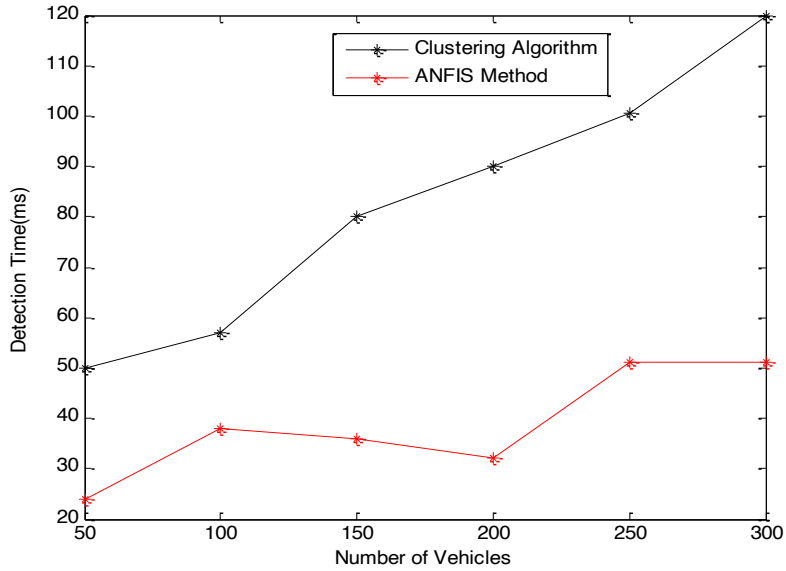


Fig. 9. False Positive Rate for Packet Drop with Number of Vehicles in total

9.2.5. Conclusion

In this paper, the authors proposed the ANFIS based detection algorithm for the security index in VANET. The proposed method will train the data internally with the neural networks and output is given to the fuzzy logic system to detect the security index. The parameters considered in this method are detection time, positive ratio, forwarding attacks with packet ratio, and the total numbers of vehicles. The proposed method will deliver better performance, with a detection rate of around 98.5%. Hence the detection rate is higher in the proposed method. Considerably detection time is even low in comparison with the existing clustering method. The detection time is around 25 secs for 50 vehicles and 52 secs for 300 vehicles. All-inclusive, the proposed approach results in better performance. The limitation of proposed method is; it takes more time to train the neural networks in ANFIS system.

9.3. Reinforcement Algorithm based Jamming-Detection for Vehicular Ad Hoc Networks

This paper focuses on third objective "Developing a model for detecting and distinguishing jamming attack in VANET". The authors proposed the reinforcement learning algorithm for the detection of jamming attacks. This algorithm as the advantages of maximizes the performance and it will sustain for a long time. In the proposed will give the better detection for jamming attacks with comparison of existing methods.

9.3.1. Classification Of Behaviors Based On Its Types

The proposed classification reinforcement algorithm and random forest will classify the different types of misbehavior in VANET. The behavior types in to four types.

The four types are classified as follows:

1. Geographical Position Validation
2. Received Signal Strength
3. Speed Deviation Detection
4. Acceptance Range Detection wrt RSU.

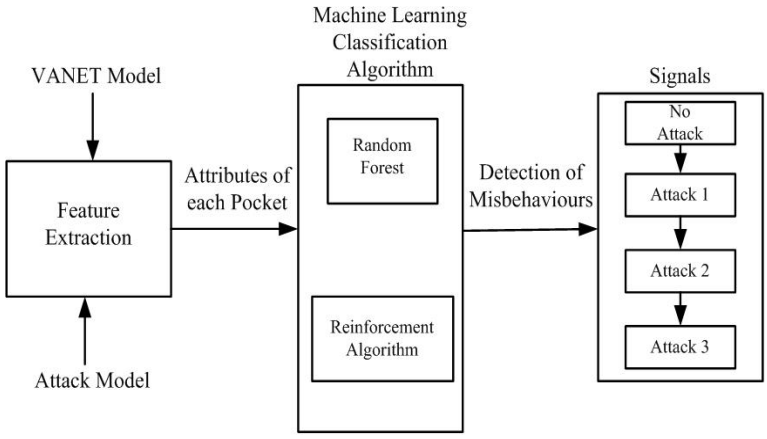


Fig. 10. Proposed Design for Classification Nodes

The Temporal Attacks are detected and classify by safety pocket distribution behavior with parameters like packets received, numbers of packets transmitted, number of packets dropped, and number of packets captured.

The object in the environment with finite state of actions decides to take decision randomly from all possible solutions for its present state. The probability of the agent reaching the target state guided by its previous state. So, in the reinforcement learning algorithm the future strategy is depends on the existing and previous states. The Reinforcement learning algorithms are used to solve Markov Decision process.

The detection of jamming attacks will be based on the packet delivery time. That means the packet delivery time is not happened in time then it will be misbehavior is happened. If the packet delivery has appeared in time, then there is no jamming and messages will pass perfectly to the vehicles.

9.3.2. Markov Decision process: Reinforcement Learning:

Reinforcement Learning is a type of Machine Learning. It allows machines and software agents to automatically determine the ideal behavior within a specific context, to maximize its performance. Simple reward feedback is required for the agent to learn its behavior; this is known as the reinforcement signal.

There are many different algorithms that tackle this issue. As a matter of fact, Reinforcement Learning is defined by a specific type of problem, and all its solutions are classed as Reinforcement Learning algorithms. In the problem, an agent is supposed to decide the best action to select based on his current state. When this step is repeated, the problem is known as a Markov Decision Process**.**

A Markov Decision Process (MDP) model contains:

- A set of possible world states S.
- A set of Models.
- A set of possible actions A.
- A real valued reward function R(s,a).
- A policy the solution of Markov Decision Process**.**
-

The main objective of Markov decision process is to find the policy function π(s) which is stores the values of actions. The term V(s) is storing the values in the first array.The equations of π(s) and V(s) is given by the Eq. (1) and Eq.(2).

$\pi(s) = argmax\ \{sT\_a\ (s, a`)(R\_a\ (s, s`)\gamma v(s`))\}$ (1)

$V(s) = s\_(s`)\ T\_\pi(s)\ \ (s, s`)(R\_\pi(s)\ \ (s, s`) + \gamma v(s`))$ (2)

The optimal values of π(s) and V(s) is given by the Eq. (3) and Eq. (4).

$\pi\hat{} * \ (s) = \ SES\ arg[max\pi\ V\hat{}\pi\ (s)]$ (3)

$V\hat{} * \ (s) = Max\pi\ V\hat{}\pi\ (s)$ (4)

Depending upon the Eq. (1) and Eq. (2) the algorithm dividedinto two algorithms. Namely first one is value iteration algorithm and second one is policy iteration.

- Value Iteration: The value iteration algorithm is the value function with iterated and π(s) is calculated and get the value using V(s).

- Policy Iteration : The policy iteration needs to observe the converges of V^* (s) and calculated the π^* (s) by using the set of linearequations.

- Q-Learning : The Q-value is defined as the sum of reinforcement parameters i.e., is intermediate and future rewards updated during learning algorithm. The action for the Q-function is called as the Q-Learning [22]. The algorithm must convergethe optimal values with the probability is 1. Due this Q- Learning is most effective for the classification type applications. The flowchart for Q-learning is shown in Fig.5.The formula for the value Q- is given by Eq. (5)

  $Q(s, a) = R(s, a) + \gamma * (max(Q, (s`, A))$ (5)

9.3.3. RESULTS AND DISCUSSIONS

The experimental setup has been done in MATLAB 2014. Here considered the parameters of 6 high kms with twodirection and time are varied between the 20-2000 seconds.

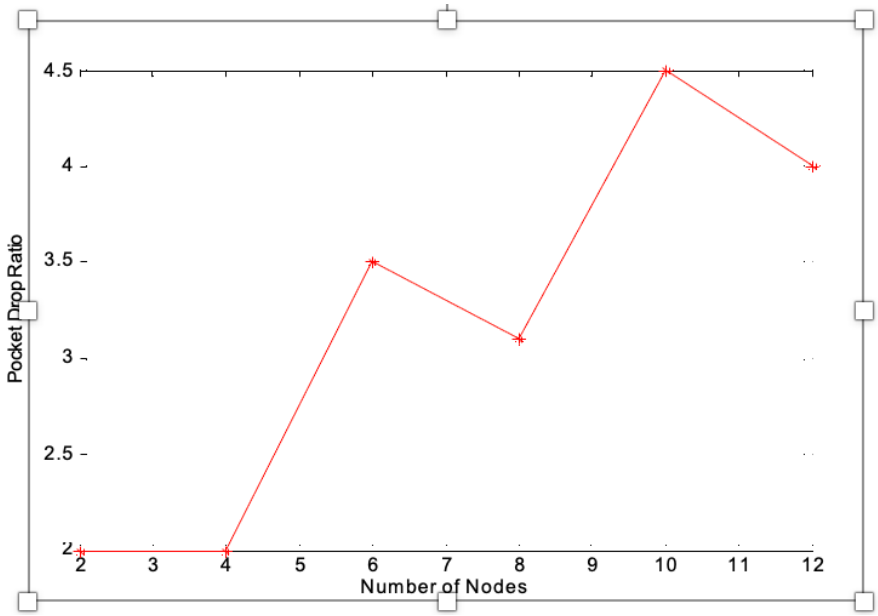
The speed variation is about 1-50m/s. The detection of jamming attack will be based on the pocket delivery time. Delay in packet delivery time is an indication of misbehavior. In time delivery of packet to destination vehicle indicates normal behavior of the network and absence of jamming in the network, If the pocket delivery has appeared in time, thenthere is no jamming and messages will pass perfectly to the vehicles.

In the proposed reinforcement learning algorithm will train the jamming detection and no jamming detection with help of predefined data. If the new data is applied to the algorithm, will detect exactly whether misbehavior is happened or not. The Reinforcement algorithm will have better results than the random forest and naïve bayes algorithms. The Results is shown in Table.2. In the fig.11. shows the packet delivery ratio with Nodes. The proposed algorithm will give the best rate of packetdrop when jammer is placed.

Classification Algorithm	True Ratio	False Ratio
Naive Bayes	0.42	0.03
Random Forest	0.92	0.01
Reinforcement Learning Algorithm	0.925	0.01

Table 2: Comparison Table for Classification of Jamming Detection

Figure 11 shows the packet drop by jammer with the packetdrop



9.3.4. Conclusion

In this paper, authors proposed the reinforcement learning algorithm for the detection of jamming network. The reinforcement algorithm produces the results according to thepartly data and with probability 1. Reinforcement algorithm has three steps with Markov Decision Process, value iteration, policy iteration and Q-learning algorithm. The detection of jamming based on the packet drop ratio with respect to nodes. The proposed system is compared with existing algorithms like Random Forest, Naïve Bayes classification algorithms. The proposed Reinforcement will produce the better solution and fast detection of Jamming Attacks in the VANETS.

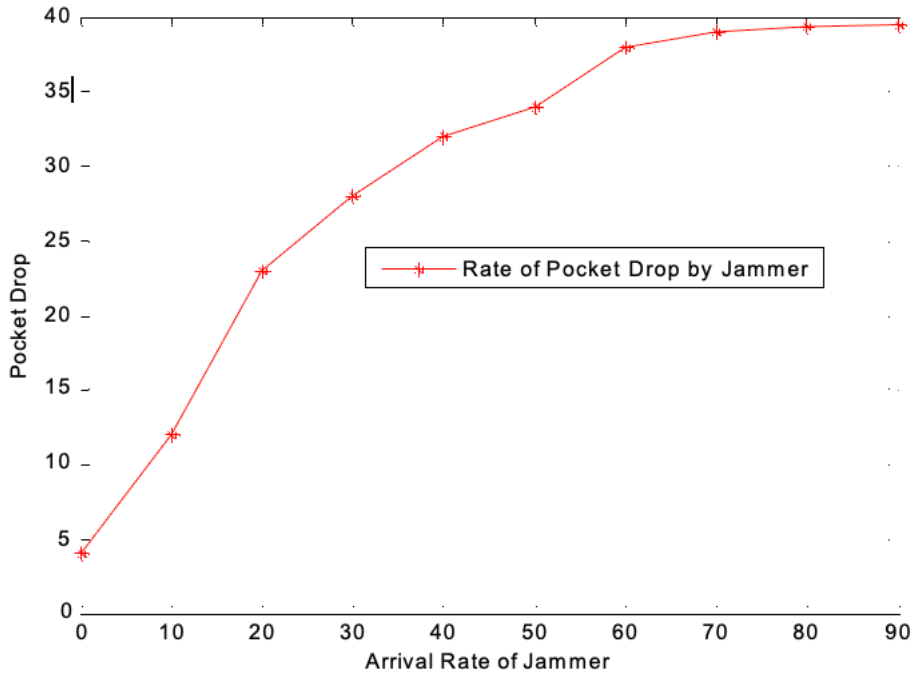


Fig 12: Rate of Packet Drop by Jammer

9.4. Multi-Layer Perceptron based Fuzzy Logic Technique for detection of Attacks in VANETs

This paper focuses on third objective "Developing a model for detecting and distinguishing jamming attack inVANET". Here we have proposed a method that uses artificial intelligence. The proposed method is the combination of Neural Network based Multilayer Perceptron (MLP) trained Fuzzy Logic System procedure to spot unusual behavior of automobiles in the ad hoc network. To validate results, variables such as detection time, detection ratio, and positive false ratio are used. The outcome of the presented method is finer in comparison to existing methods.

9.4.1. Methods and Tools

The proposed work is to aim at the deep learning-based multi-layer perceptron network (mlp) trained fuzzy logic controller to obtain the security index in the vehicular network. further explanation of proposed method with techniques used is presented in depth. the proposed method is a combination of neural networks and fuzzy logic techniques. in this method, initially, data is trained using advanced deep learning techniques like MLP and backpropagation algorithms. later, prepared data is used for fuzzy logic to detect the index of attacks. the first fuzzy logic is introduced in [18]. There are various algorithms available such as supervised and unsupervised algorithms. The other method of preparing the data is using Back Propagation Algorithm and Multi-Layer Perceptron methods.

9.4.1. Output And Explanation

In VANET, its execution with reliability has significant importance. The proposed method has evolved with both Neural Network Type Multilayer Perceptron (MLP) The proposed method has a simple design and will give better performance.

Performance Evolution

To evaluate the proposed method, three parameters are considered: rate of detection, false-positive rate, time to detect in opposition to packet ratio, and selective forwarding attacks.

Detection Rate:

This is the count of suspicious incident's ratio announced to the occurrences of count of suspicious incident.

DR = (malicious events Detected in total) / (malicious events in total)

If the DR is high, then the accuracy of the detection system is also more.

False positive rate (FPR):

This denotes the proportion of a fake obstruction noticed to the count of standard point.

FPR = Innocent Nodes Detected in total /standard nodes in total.

Parameters	Values
Apparatus to simulate	NetSim and MATLAB
Traffic Generator	SUMO
Range of Communication	250 m
MAC Protocol	IEEE 802.11 p
Node Density	50–300
Simulation Area	300 m × 300 m
Type of Connection	UDP
Type of Application	CBR
Size of Packet	512 bytes
Highest. no. of Suspicious Nodes	45% of the total Nodes
Time to Simulate	700 s
Mobility Model	Manhattan Mobility Model
Types of Attack	Packet Drop, Selective Forwarding

The proposed system's performance is depicted in the waveform. Figure 13 gives the performance of detection rate with the proposed method and existing clustering method [22].

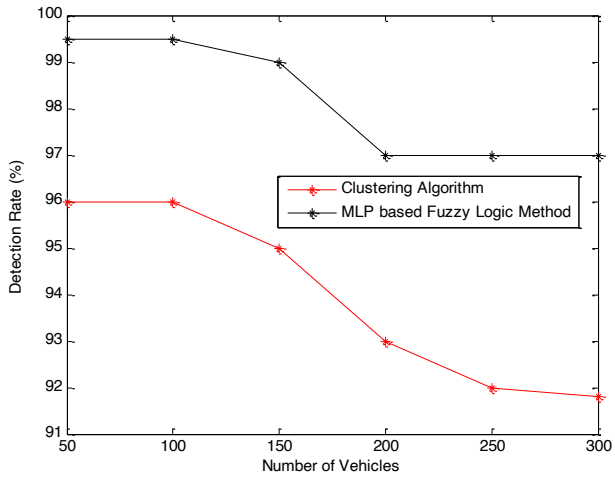


Fig.13: Performance of Detection Rate with Proposed and Existing Method

As the detection rate goes high, the system will result in better performance. The proposed MLP based Fuzzy logic method results in a high detection rate, around 23%, with the 50 vehicles. For 300 vehicles, the rate of detection in the current work is 97.5%. Hence in comparison with existing methods, the proposed method has an elevated detection rate.

Figure.14 shows the performance of the number of vehicles with a False positive ratio for existing and proposed methods. The False positive rate is low for each number of vehicles in the proposed work. In contrast, current practices have a higher false-positive ratio than the number of vehicles in comparison with present work.

Figure .15 exhibits performance of detection time in the proposed method and existing methods with the positive forward attack. The proposed method has less detection time with the number of vehicles. The clustering algorithm [22] shows the performance with high detection time. In conclusion, the proposed method manifests better performance with the above results.

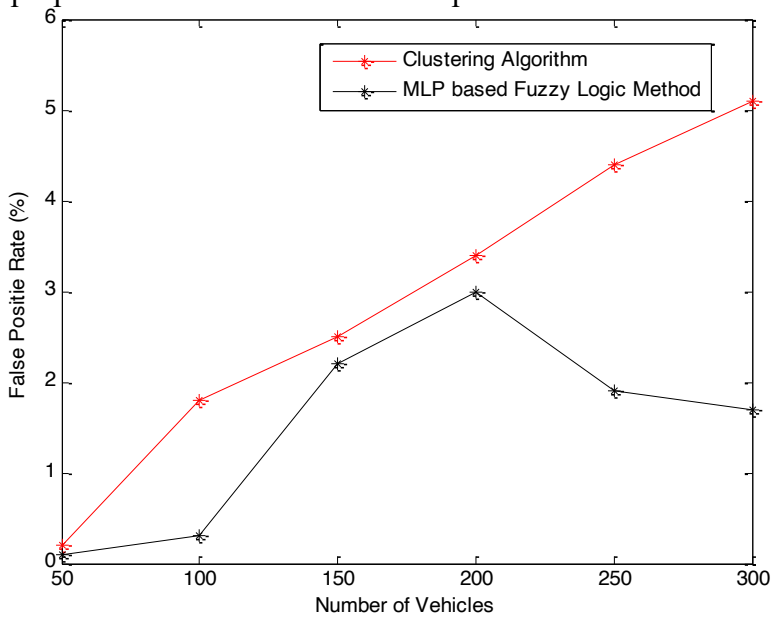


Fig.14: False Positive Rate for Packet Drop with no. of vehicles

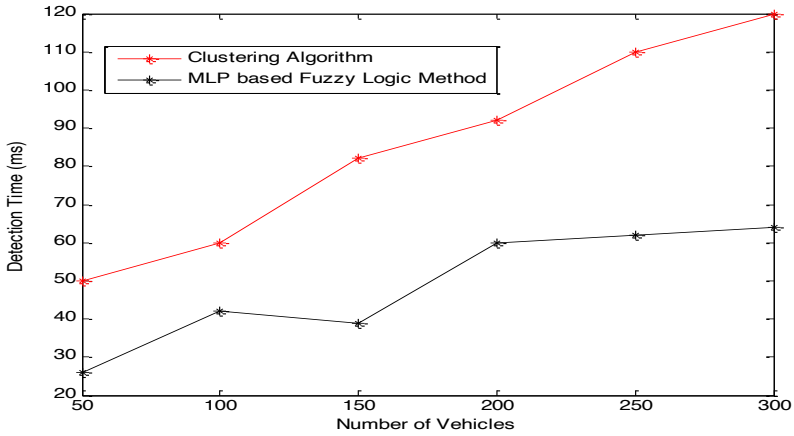


Fig.15:. False Positive Rate for Packet Drop with Number of Vehicles in total

9.4.2. Conclusion

In this paper, the authors proposed the MLP based Fuzzy Logic method that detects the attack in the system. Data is fed to MLP to train them. The Error Back Propagation Algorithm (BPA) will be acclaimed to prepare the data. As the BPA system produces the minimum amount of error, it will stop the training of data. Membership functions that are high, medium, low are given to the Fuzzy logic system based on minimum error obtained from trained data.

The proposed method will deliver better performance, with a detection rate of around 98%. Hence the detection rate is higher in the proposed method. Considerably detection time is even low

in comparison with the existing clustering method. The detection time is around 27 sec for 50 vehicles and 55 sec for 300 vehicles: All-inclusive, the proposed approach results in better performance.

9.5. Comparison of different AI based Techniques for the detection of Jamming Attacks in VANETS

This paper focuses on the fourth objective "Comparative analysis of jamming attack detection technique." In this paper authors are analyzed the different types of Artificial Intelligence Techniques which is used in the Jamming detection of VANETs. The AI based techniques have different advantages due to its pre training of data. Here authors are compared the three different techniques which is used in jamming detection.

9.5.1. Methods for Detection of Jamming Attacks in VANETS

Artificial Intelligence, machine learning classification algorithm like Random Forest, Reinforcement Learning Algorithm and Deep learning Algorithms like Neural Networks and Adaptive Neuro fuzzy Algorithms produces their own results like human beings

9.5.2. Reinforcement Learning Algorithm

The Reinforcement learning is the important algorithm in the part of the machine learning system algorithms which has been developed with the concept of the living learning and real life environment situations [8-9]. The object in the environment with finite state of actions decides to take decision randomly from all possible solutions for its present state. The probability of the agent reaching the target state guided by its previous state. So, in the reinforcement learning algorithm the future strategy depends on the existing and previous states. The Reinforcement learning algorithms are used to solve Markov Decision process.

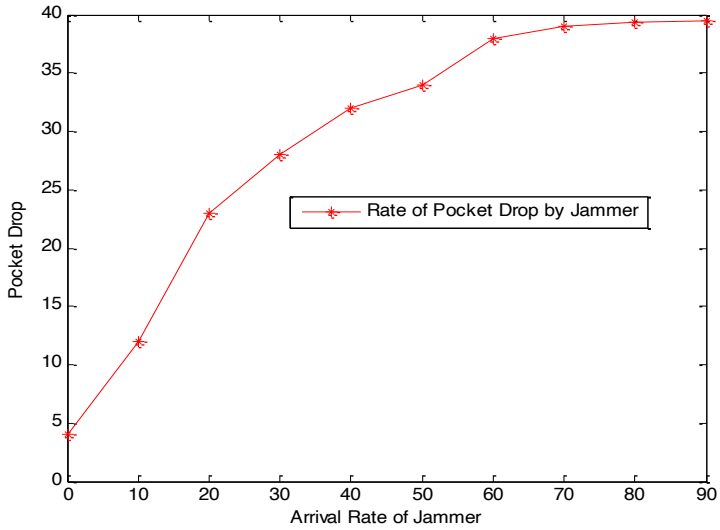


Fig 16: Rate of Packet Drop by Jammer

The Figure. 16 shows the jamming detection parameter pocket ratio in VANETs using reinforcement learning algorithm.

9.5.3. Multi-Layer Perceptron based Fuzzy Logic Technique

The deep learning-based multi-layer perceptron network (MLP) trained fuzzy logic controller to obtain the security index in the vehicular network. further explanation of proposed method with techniques used is presented in depth. the proposed method is a combination of neural networks and

fuzzy logic techniques. in this method, initially, data is trained using advanced deep learning techniques like MLP and back propagation algorithms. later, prepared data is used for fuzzy logic to detect the index of attacks [11]. The Figure .17 shows the results the results of multilayer perceptron methods.

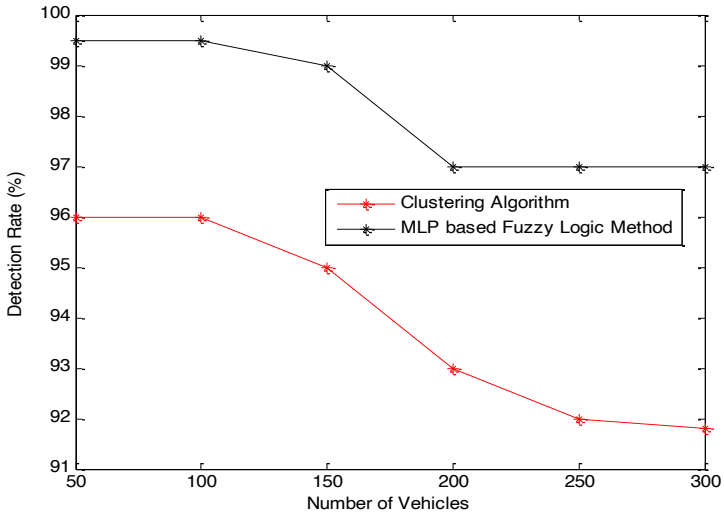


Fig 17: Performance of Detection Rate with MLP Fuzzy Logic Method

9.5.4. ANFIS based Jamming Detection

It is mixture of ANN with fuzzy interface system. The Takagi - Sugeno model is used in this proposed work. ANFIS is a very good learning technique to take over an issue on uncertainties in any system. This controller is based on framing fuzzy IF-Then rules that produces specific input-output with the help of membership functions. The learning process of ANFIS consists of three stages; first is the rule base, second is the membership functions and the third is the reasoning mechanism [12]. The Figure .18 shows the results the results of multilayer perceptron methods.

If Vj= If x1 is A1(x1) and x2 is A2j(x2) and .....xn is Anj (xn) THEN y is cj. Here x1 is considered as change in error given as wref- wr and x2= derivative of change in error given as d(wref- wr)/dt.. Output is defined by the formula y = output given as Pix1+Rix2+Si.

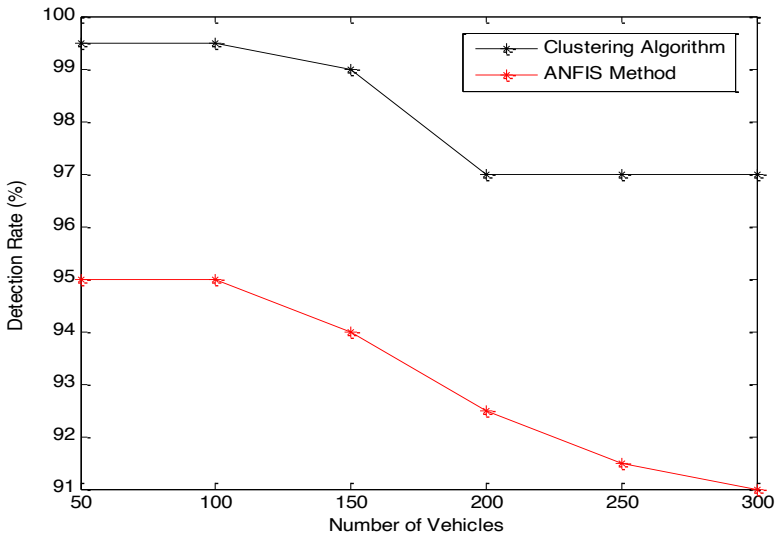


Fig 18.: Performance of Detection Rate with ANFIS Method

9.5.5. Conclusions

In this paper, the authors compared the Reinforcement methods, MLP- Fuzzy Logic method and ANFIS Methods. The parameters used here are detection time, positive ratio, forwarding attacks with packet ratio, and the total numbers of vehicles are considered. The MLP- Fuzzy Logic and ANFIS methods will give the better performance.

10. PUBLICATION WORK DONE

SL.NO	OBJECTIVE	PAPER TITLE	JOURNAL	INDEX	STATUS
1	Survey & Investigating detection mechanisms for jamming attack in VANET	A Comprehensive Study of Security Attack on VANET	SPRINGER (ISSN 2367-4512 ISSN 2367-4520 (electronic) Lecture Notes on Data Engineering and Communications Technologies ISBN 978-981-16-2936-5 ISBN 978-981-16-2937-2 (eBook) https://doi.org/10.1007/978-981-16-2937-2)	SCOPUS	PUBLISHED
2	Performance analysis of detection techniques for jamming attack.	Adaptive Neuro Fuzzy Technique for Jamming Detection in VANETs	SPRINGER	SCOPUS	ACCEPTED
3.	Developing a model for detecting and distinguishing jamming attack in VANET	Reinforcement Algorithm based Jamming-Detection for Vehicular Ad Hoc Networks	IEEE (978-1-6654-1758-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/IBSSC53889.2021.9673350)	SCOPUS	PUBLISHED
		Traffic Jam Detection Using Regression Model Analysis on IoT-Based Smart City	IEEE Advances in Data-driven Computing and Intelligent Systems (ADCIS 2022)	SCOPUS	ACCEPTED
4.	Comparative analysis of jamming attack detection technique.	Traffic Jam Detection Using Regression Model Analysis on IoT-Based Smart City	IISTEM(International Institution for Science Technology Engineering and Management)	DRJI, Google Scholar	ACCEPTED

11. CONCLUSION

VANET is promising technology for vehicular communication network, due to its extensive applications and vivid safety related services. It has undoubtedly become a topic of research in the field of automobile, educational institution etc. Due to gaining popularity of VANET, security and attack has become major concern. Dealing with various attacks like jamming is a challenging task.

Hence maximizing road safety and minimizingjamming attack on vehicles, which hinders communication between vehicles is the major concern. Focus of the research work is on detecting the jamming attack and analyzing performance of VANET under different scenarios. Detecting and preventing jamming in VANET will ultimately enhance road safety and in time message delivery between vehicles.

12. FUTURE SCOPE

As known VANET is a wireless technology which do not remain constant. It is a growing technology, wherein which each stage of technology upgrading is facing new challenges concerned to the security. However, there is a wide scope of improvement in models developed in our research work. The efficiency and jamming detection rate can be fine-tuned with other / new models.

Diverse techniques have been implied to locate the jamming in VANET, which is a challenge. Exploring existing techniques which have prominently identified and resolved jamming becomes a base to make a in depth study about the issue and to come up witha model which can work more efficiently

13. REFERENCE

[1] Anis Laouiti, Amir Qayyum, and Mohamad Naufal Mohamad Saad. Vehicular Ad-hoc Networks for Smart Cities: First International Workshop, 2014, volume 306. Springer, 2014.

[2] Rakesh Shrestha, Rojeena Bajracharya, and Seung Yeob Nam. Challenges of future vanet and cloud-based approaches. Wireless Communications and Mobile Computing, 2018, 2018.

[3] Wenjia Li and Houbing Song. Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 17(4):960 969, 2016.

[4] Furqan Jameel, Zara Hamid, Farhana Jabeen, and Muhammad Awais Javed. Impact of co-channel interference on the performance of vanets under α-μ fading. AEU-International Journal of Electronics and Communications, 83:263 269, 2018.

[5] Shahid Latif, Saeed Mahfooz, Bilal Jan, Naveed Ahmad, Yue Cao, and Muham- mad Asif. A comparative study of scenario-driven multi-hop broadcast protocols for vanets. Vehicular Communications, 2018.

[6] D Dinesh and M Deshmukh. Challenges in vehicle ad hoc network (vanet). International Journal of Engineering Technology, Management and Applied Sciences, 2(7):76 88, 2014.

[7] Anil D Devangavi and Rajendra Gupta. Routing protocols in vanet a survey. In Smart Technologies For Smart Nation (SmartTechCon), 2017 International Conference On, pages 163 167. IEEE, 2017.

[8] Raju Barskar and Meenu Chawla. Vehicular ad hoc networks and its applications in diversi ed elds. International Journal of Computer Applications, 123(10), 2015.

[9] Wedad Ahmed and Mourad Elhadef. Securing intelligent vehicular ad hoc networks: A survey. In Advances in Computer Science and Ubiquitous Computing, pages 6 14. Springer, 2017.

[10] Nnanna Ekedebe, Wei Yu, Chao Lu, Houbing Song, and Yan Wan. Securing transportation cyber-physical systems. In Securing Cyber-Physical Systems, pages 163 196. CRC Press, 2015.

[11] Abderrahim Benslimane and Huong Nguyen-Minh. Jamming attack model and detection method for beacons under multichannel operation in vehicular networks. IEEE Transactions on Vehicular Technology, 66(7):6475 6488, 2017.

[12] Sharaf Malebary, Wenyuan Xu, and Chin-Tser Huang. Jamming mobility in 802.11 p networks: Modeling, evaluation, and detection. In Performance Computing and Communications Conference (IPCCC), 2016 IEEE 35th International, pages 1 7. IEEE, 2016.

[13] Dimitrios Karagiannis and Antonios Argyriou. Jamming attack detection in a pair of rf communicating vehicles using unsupervised machine learning. Vehicular Communications, 13:56 63, 2018.

[14] Ferdinand Nyongesa, Karim Djouani, T Olwal, and Yskandar Hamam. Doppler shift compensation schemes in vanets. Mobile Information Systems, 2015, 2015.
[15] AM Abdelgader and Wu Lenan. The physical layer of the ieee 802.11 p wave communication standard: the speci cations and challenges. In Proceedings of the world congress on engineering and computer science, volume 2, page 71, 2014.
[16] Humeng Lv, Xuemei Ye, Li An, and Yuan Wang. Distributed beacon frequency control algorithm for vanets (dbfc). In Intelligent System Design and Engineering Application (ISDEA), 2012 Second International Conference on, pages 243 246. IEEE, 2012.
[17] Yi Qian, Kejie Lu, and Nader Moayeri. A secure vanet mac protocol for dsrc applications. In Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, pages 1 5. IEEE, 2008.
[18] Huong Nguyen-Minh, Abderrahim Benslimane, and Abderrezak Rachedi. Jamming detection on 802.11 p under multi-channel operation in vehicular networks. In Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on, pages 764 770. IEEE, 2015.
[19] Sara Orn Tengstrand, Karina Fors, Peter Stenumgaard, and Kia Wiklundh. Jam- ming and interference vulnerability of ieee 802.11 p. In Electromagnetic Compatibility(EMC Europe), 2014 International Symposium on, pages 533 538. IEEE, 2014.
[20] Ali Hamieh, Jalel Ben-Othman, and Lynda Mokdad. Detection of radio interference attacks in vanet. In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pages 1 5. IEEE, 2009.
[21] Ram Shringar Raw, Manish Kumar, and Nanhay Singh. Security challenges, issues and their solutions for vanet. International Journal of Network Security & Its Applications, 5(5):95, 2013.
[22] Nikita Lyamin, Alexey Vinel, Magnus Jonsson, and Jonathan Loo. Real-time detection of denial-of-service attacks in ieee 802.11 p vehicular networks. IEEE Communications letters, 18(1):110 113, 2014.
[23] Ikechukwu K Azogu, Michael T Ferreira, Jonathan A Larcom, and Hong Liu. A new anti-jamming strategy for vanet metrics-directed security defense. In 2013 IEEE Globecom Workshops (GC Wkshps), pages 1344 1349. IEEE, 2013.
[24] Amer Aijaz, Bernd Bochow, Florian Dotzer, Andreas Festag, Matthias Gerlach, Rainer Kroh, and Tim Leinmuller. Attacks on inter vehicle communication systems-an analysis. Proc. WIT, pages 189 194, 2006.
[25] Mingshun Sun, Ming Li, and Ryan Gerdes. A data trust framework for vanets enabling false data detection and secure vehicle tracking. In 2017 IEEE Conference on Communications and Network Security (CNS), pages 1 9. IEEE, 2017.
[26] Muhammet Ali Karabulut, AFM Shahen Shah, and Haci Ilhan. Performance modeling and analysis of the ieee 802.11 dcf for vanets. In 2017 9th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pages 346 351. IEEE, 2017.